Listing of Claims:

1. (Original) A method for preventing identity theft in electronic communications, comprising the steps of:

sequencing an encryption key transaction from a trusted service for generating for an individual a consumer identifier by performing the steps of:

issuing from said trusted service a primary key to the individual;

issuing to the individual a unique identifier from said trusted service; and

permitting the individual to generate and maintain a consumer-defined sequence through said trusted service; and

allowing the individual to control access to commercially related use of said consumer identifier by third parties.

2. (Original) The method of Claim 1, further comprising the steps of verifying commercially related use of said consumer identifier, comprising the steps of:

initiating a verification process from a requesting business entity via a secure connection;

comparing said consumer identifier with a pre-determined set of database records using said consumer-defined sequence in response to initiating said verification process;

presenting a positive or negative confirmation to said requesting business, said business having registered with said trusted service; and

confirming requested information relating to the individual via said secure connection, said requested information have been pre-authorized for presenting to said requesting business entity by the individual.

3. (Original) The method of Claim 2, further comprising the step of reporting to the individual the number of times at least one requesting business entity has initiated a verification process.

4. (Original) The method of Claim 2, further comprising the step of confirming requested information relating to the individual including the individual's name, address, and photograph.

5. (Original) The method of Claim 2, further comprising the step of confirming requested information relating to the individual including the individual's fingerprints.

6. (Original) The method of Claim 1, further comprising the steps of storing said consumer identifier on a remote business database system and permitting the individual to modify said consumer identifier through a secure connection to a remote location.

7. (Original) The method of Claim 1, further comprising the step of issuing to the individual a unique identifier from said trusted service according to a pre-determined set of business rules associated with a remote business database system.

8. (Original) The method of Claim 1, further comprising the step of allowing the individual to control commercial transactions using said consumer identifier.

9. (Original) The method of Claim 1, further comprising the step of issuing to the individual a unique identifier from said trusted service, said unique identifier conveying in encrypted information relating to the individual's age and locale.

10. (Previously Presented) A system for preventing identity theft in electronic communications, comprising:

instructions stored on a computer-readable medium for sequencing an encryption key transaction from a trusted service for generating for an individual a consumer identifier, said sequencing instructions, further comprising:

instructions for issuing from said trusted service a primary key to the individual;

instructions for issuing to the individual a unique identifier from said trusted service; and

instructions for permitting the individual to generate and maintain a consumer-defined sequence through said trusted service; and

instructions stored on a computer-readable medium for allowing the individual to control access to commercially related use of said consumer identifier by third parties.

11. (Previously Presented) The system of Claim 10, further comprising instructions stored on a computer-readable medium for verifying commercially related use of said consumer identifier, comprising:

instructions for initiating a verification process from a requesting business entity via a secure connection;

instructions for comparing said consumer identifier with a pre-determined set of database records using said consumer-defined sequence in response to initiating said verification process;

instructions for presenting a positive or negative confirmation to said requesting business, said business having registered with said trusted service; and

instructions for confirming requested information relating to the individual via said secure connection, said requested information have been pre-authorized for presenting to said requesting business entity by the individual.

12. (Previously Presented) The system of Claim 11, further comprising instructions stored on a computer-readable medium for reporting to the individual the number of times at least one requesting business entity has initiated a verification process.

13. (Previously Presented) The system of Claim 11, further comprising instructions stored on a computer-readable medium for confirming requested information relating to the individual including the individual's name, address, and photograph.

14. (Previously Presented) The system of Claim 11, further comprising instructions stored on a computer-readable medium for confirming requested information relating to the individual including the individual's fingerprints.

15. (Previously Presented) The system of Claim 10, further comprising instructions stored on a computer-readable medium for storing said consumer identifier on a remote business database system and permitting the individual to modify said consumer identifier through a secure connection to a remote location.

16. (Previously Presented) The system of Claim 10, further comprising instructions stored on a computer-readable medium for issuing to the individual a unique identifier from said trusted service according to a pre-determined set of business rules associated with a remote business database system.

17. (Previously Presented) The system of Claim 10, further comprising instructions stored on a computer-readable medium for allowing the individual to control commercial transactions using said consumer identifier.

18. (Previously Presented) The system of Claim 10, further comprising instructions stored on a computer-readable medium for issuing to the individual a unique identifier from said trusted service, said unique identifier conveying in encrypted information relating to the individual's age and locale.

19. (Previously Presented) A computer-readable storage medium comprising a system for preventing identity theft in electronic communications, comprising:

instructions stored on said storage medium for sequencing an encryption key transaction from a trusted service for generating for an individual a consumer identifier, said sequencing instructions, further comprising:

instructions stored on said storage medium for issuing from said trusted service a primary key to the individual;

instructions stored on said storage medium for issuing to the individual a unique identifier from said trusted service; and

instructions stored on said storage medium for permitting the individual to generate and maintain a consumer-defined sequence through said trusted service; and

instructions stored on said storage medium for allowing the individual to control access to commercially related use of said consumer identifier by third parties.

20. (Previously Presented) The computer-readable storage medium of Claim 19, further comprising, as a part of said identity theft prevention system, instructions stored on said storage medium for verifying commercially related use of said consumer identifier, said verifying instructions comprising:

instructions stored on said storage medium for initiating a verification process from a requesting business entity via a secure connection;

instructions stored on said storage medium for comparing said consumer identifier with a pre-determined set of database records using said consumer-defined sequence in response to initiating said verification process;

instructions stored on said storage medium for presenting a positive or negative confirmation to said requesting business, said business having registered with said trusted service;

instructions stored on said storage medium for confirming requested information relating to the individual via said secure connection, said requested information have been pre-authorized for presenting to said requesting business entity by the individual.